Surveying Cyberspace

Cybersecurity

Cybersecurity 101 Day 2

Class Objectives

By the end of today's class, you will be able to:

- Articulate a clear definition of the CIA triad and its elements.
- Define and contextualize technical terms found in recent cybersecurity trends and reports.
- Use cybersecurity trend reports to communicate risk patterns.
- Conduct and present analysis on a vulnerability, exploit, or threat actor to a non-technical audience using independent research.

Let’s do a quick review!

Quick Review

Last class, we described cybersecurity as centering on **two concepts**.

What were they?

Quick Review

The **two concepts** that cybersecurity is centered on are:

- **Threat assessment**
- **Risk mitigation**

Quick Review

How would you define these terms?

- Threat assessment
- Risk mitigation

Quick Review

Threat assessment:

Structured process of identifying the risks posed to a group or system.

Risk mitigation:

Systematic reduction of the impact and/or likely occurrence of a negative event.

Quick Review

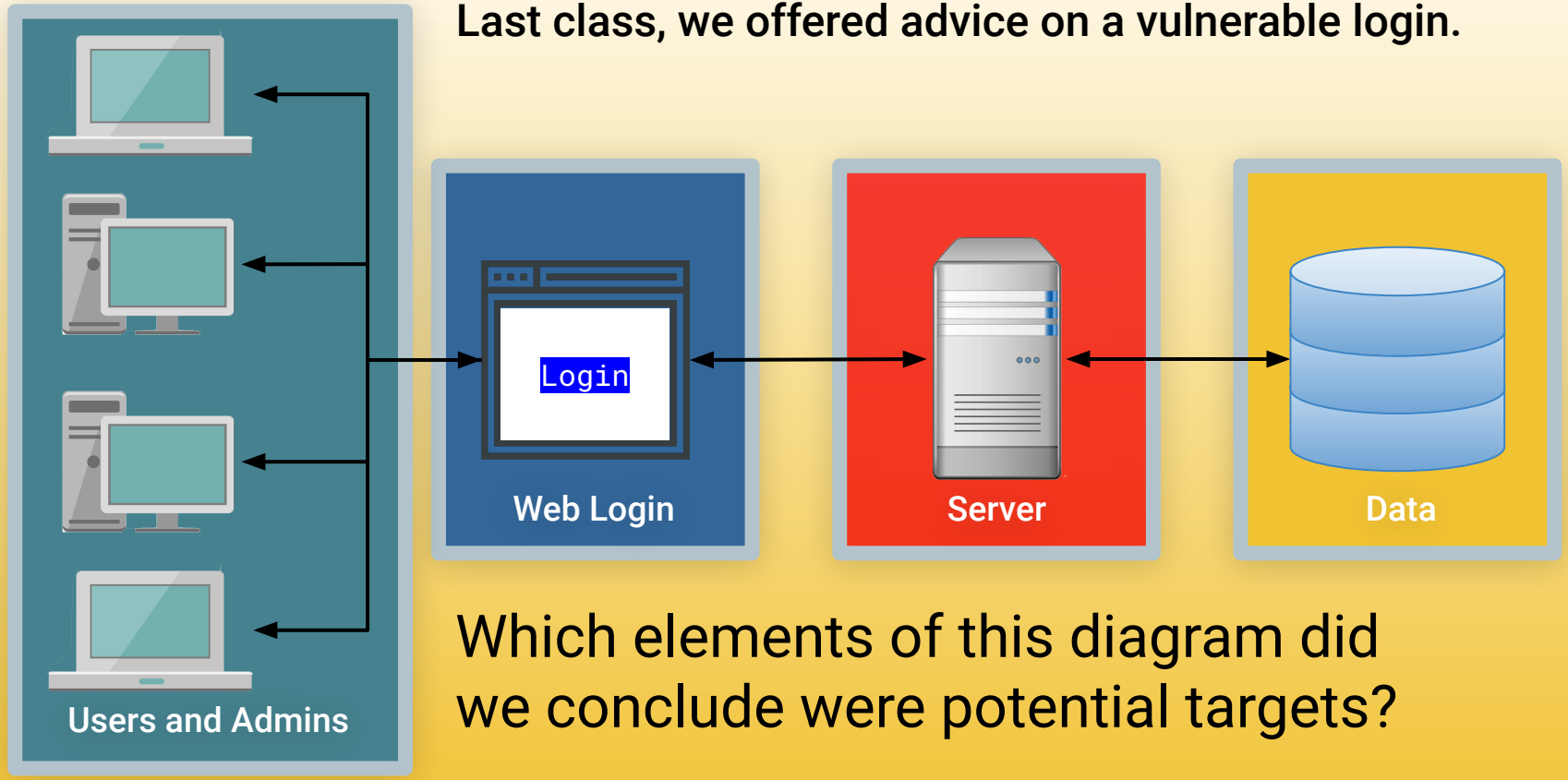
In other words...

Threat assessment:
What could happen?

Risk mitigation:
How do we handle It?

Quick Review

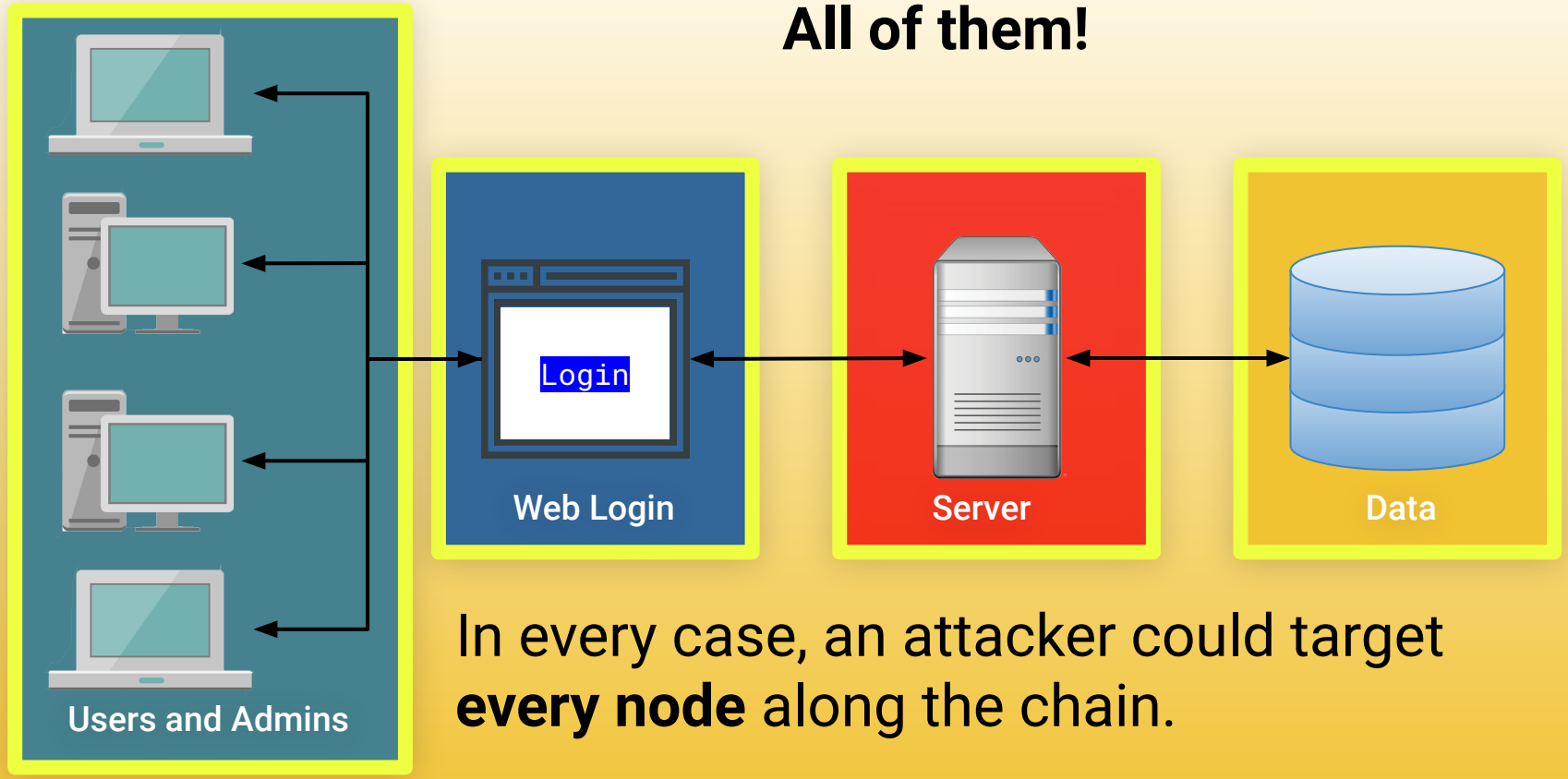
Last class, we offered advice on a vulnerable login.



Which elements of this diagram did we conclude were potential targets?

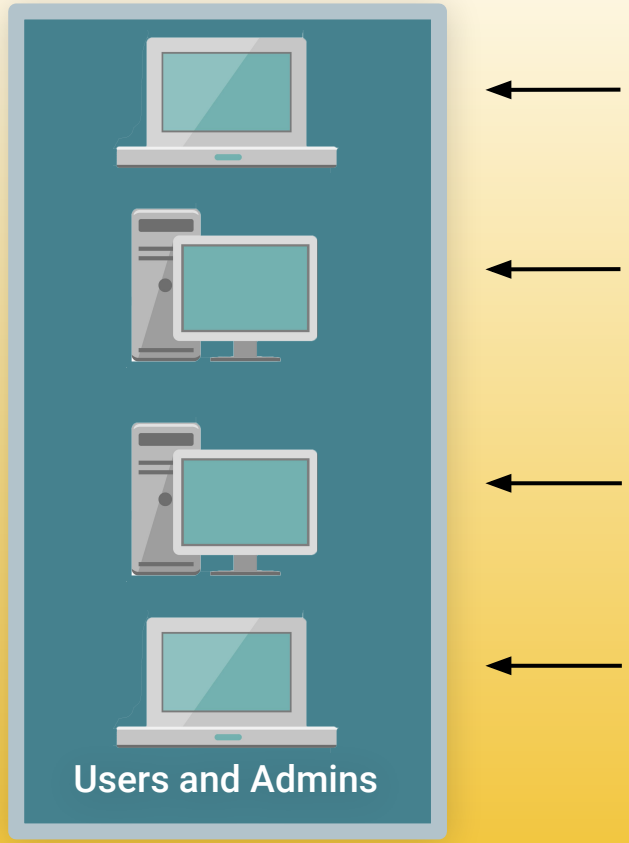
Quick Review

All of them!



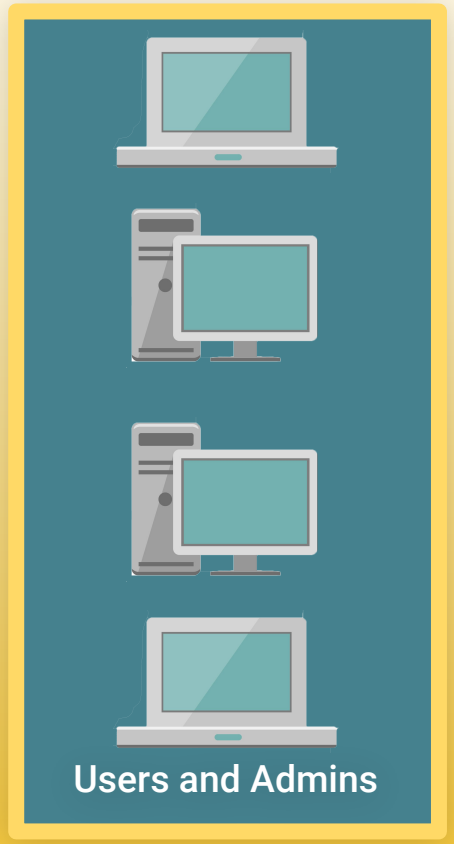
In every case, an attacker could target **every node** along the chain.

Quick Review



Name Three User Attacks

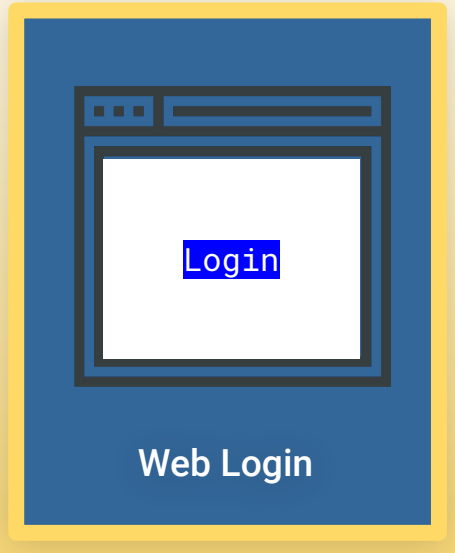
Quick Review



Name Three User Attacks

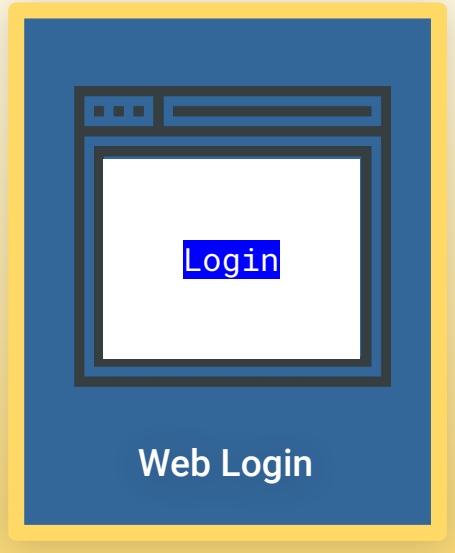
- Social Engineering
- Credential Reuse
- Malware Attacks
- Man in the Middle
- Packet Sniffing
- Computer Theft

Quick Review



Name One Website Attack

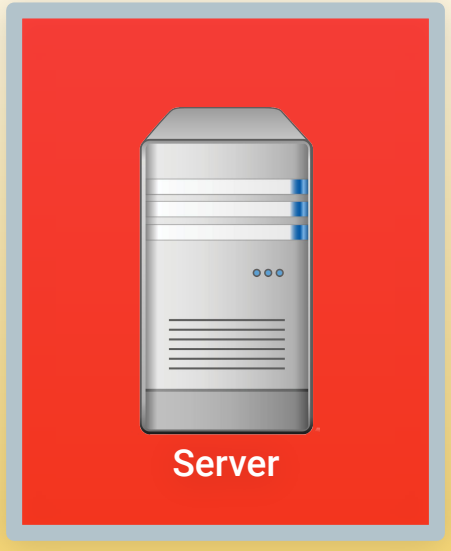
Quick Review



Name One Website Attack

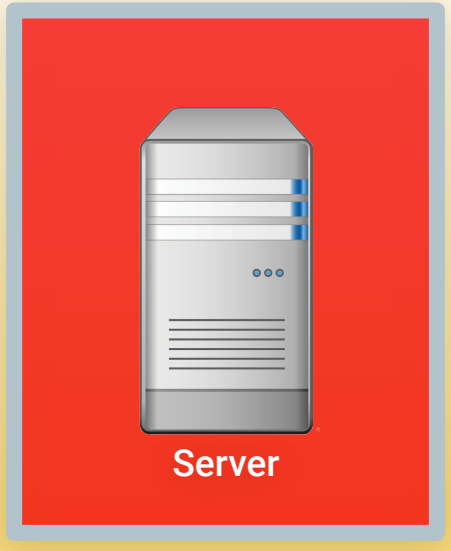
- Brute-Force Injection
- Code Injection
- Session Stealing

Quick Review



Name One Server Attack

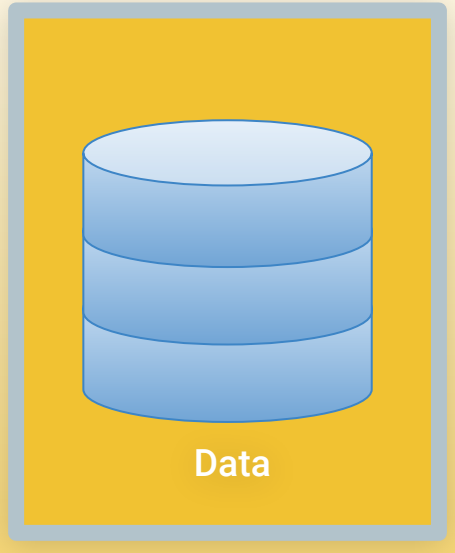
Quick Review



Name One Server Attack

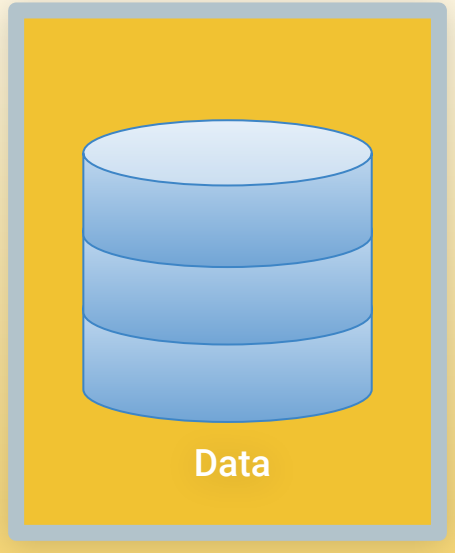
- OS Exploits
- Code Injection

Quick Review



Name One Database Attack

Quick Review



Name One Database Attack

- Default Credentials
- Unpatched Database
- Lack of Segregation

Quick Review

User Attacks

- Social Engineering
- Phishing Attacks
- Credential Reuse
- Malware Attacks
- Man in the Middle
- Packet Sniffing
- Computer Theft

Web Attacks

- Brute-Force Attacks
- Code Injection
- Faulty Sessions

Server Attacks

- OS Exploit
- Malicious Software

Database Attacks

- Default Credentials
- Unpatched Database
- Lack of Segregation

Name Three Risk Mitigation Options

Quick Review

Name Three Risk Mitigation Options

1. Educate all users on dangers of phishing and social engineering.
2. Ensure passwords are truly unique to website (require characters atypical of other websites).
3. Ensure users are using multi-factor authentication (login + phone confirmation).
4. Ensure administrators can only access the network from a secure location (on premises).
5. Ensure passwords used are *strong* (alphanumeric + symbols).
6. Ensure login fields do *not* accept any code insertions.
7. Ensure users are immediately signed off upon closing a browser.
8. Ensure all servers are routinely patched against latest known vulnerabilities.
9. Ensure physical access to servers is protected by multiple forms of authentication.
10. Ensure that all data stored in the database is encrypted and cannot be read without additional login information.
11. Ensure that all cloud security platforms follow best practices for security implementation.

Quick Review

Activity: *Oh look, a phone!*
Suppose *last class*, two students left their phones unattended at some point.

With the person next to you, **identify as many exploits as possible** that could result from a stolen cell phone.

Hint: Be creative! Think like a hacker.

- What is the worst possible damage that could happen?
- Think about *real damage*.
- Think beyond the value of the phone itself.

Quick Review

Activity Review: *Oh look, a phone!*

Potential Adverse Event

1. Cell phone can be wiped and re-sold.
2. Cell phone memory can be harvested. Photos and sensitive material could be used for blackmail.
3. Credentials for email and social media accounts could be used to extract financial gain.
4. Installed applications could be used to make purchases.
5. Malware software could be directly installed to track future activity.
6. Contacts on your phone could be socially engineered into providing monetary value.
7. Your phone could be used to conduct illegal activity.
8. Your identity could be stolen.

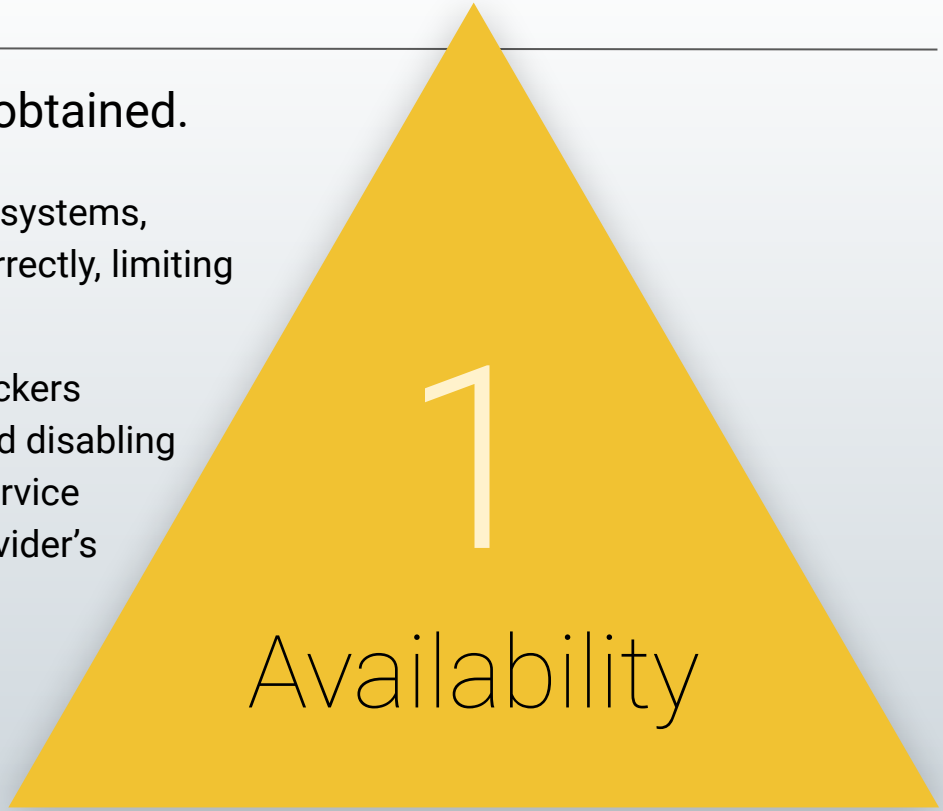
The CIA Triad

The InfoSec Bible:
The CIA Triad

Availability

The quality of being able to be used or obtained.

- Availability concerns occur when operating systems, equipment, and data are not functioning correctly, limiting accessibility to those who need it.
- Examples of availability attacks include: hackers taking down a web-connected generator and disabling a critical power supply; using a denial of service attack to bring down a financial service provider's website, making it impossible for clients to make transactions.
- Creating regular backups of data is one way to maintain availability.



Integrity

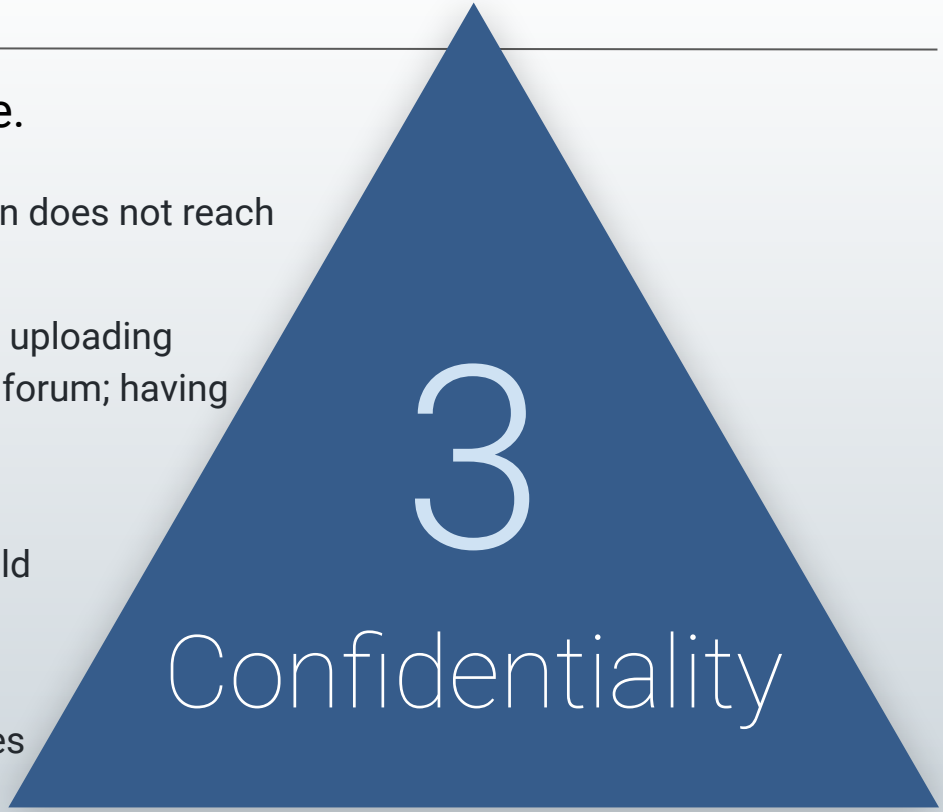
The quality of being honest, whole, or undivided.

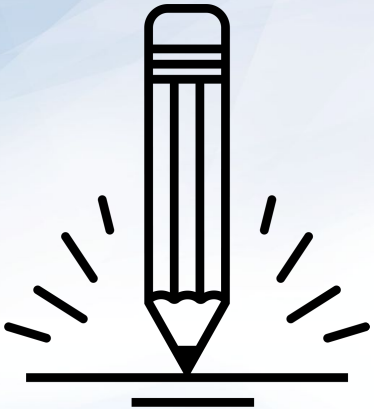
- The integrity of information refers to protecting information from being modified by unauthorized parties.
- Examples of integrity attacks include: intercepting money transfers and changing the dollar amount in “insignificant” ways in order to siphon off the excess; altering university grades to be better or worse.
- Integrity attacks can be avoided by using a secure hashing algorithm and process when transferring data to ensure it isn’t tampered with in transit.

Confidentiality

The state of being kept secret or private.

- Confidentiality ensures sensitive information does not reach unauthorized people.
- Examples of confidentiality attacks include: uploading private photos and communications onto a forum; having credit card numbers exposed online.
- Confidentiality comes down to the principle of “need to know.” Data or information should only be made available to those who need access to it.
- Confidentiality is enforced through measures like encryption and authentication.





Activity: Defending the CIA Triad

In this activity, you will analyze a variety of brief security scenarios and identify which element of the CIA triad (Confidentiality, Integrity, Availability) each situation is concerned with.

(Scenarios sent by the instructor.)

Suggested Time:
12 Minutes

Activity Instructions: Defend the CIA Triad

- A hospital only allows authorized healthcare personnel within one department access to patient Personal Identifiable Information. When employees move to another department, that access is revoked.
- A technology firm maintains an alternate site that is running at all times, and operations can be moved to this location in the event of a major disaster.
- Employees need to have key cards in order to enter their company offices.
- A company hashes their data files in order to monitor whether information has been tampered with.
- Only authorized personnel at a company have write access to certain files. All other employees have only read access to these files.
- A company employs redundant servers, which means that these systems are duplicated, and in the event of a malfunction, one server will fail over to other.
- A company's network infrastructure uses load balancers which will distribute the "load" of tasks such as file requests and data routing to a variety of servers, thereby ensuring that no single device is overburdened.
- A hacker uses a man-in-the-middle attack to intercept wireless traffic from users.
- A hacker was able to crack a hashed message and change its contents.
- A hacker launched a DDoS attack which flooded a website with unwanted traffic from a number of computers and took the site offline.

Time’s Up! Let’s Review.

Activity Instructions: Defend the CIA Triad

- A hospital only allows authorized healthcare personnel within one department access to patient Personal Identifiable Information. When employees move to another department, that access is revoked.
- A technology firm maintains an alternate site that is running at all times, and operations can be moved to this location in the event of a major disaster.
- Employees need to have key cards in order to enter their company offices.
- A company hashes their data files in order to monitor whether information has been tampered with.
- Only authorized personnel at a company have write access to certain files. All other employees have only read access to these files.

Activity Instructions: Defend the CIA Triad

- A hospital only allows authorized healthcare personnel within one department access to patient Personal Identifiable Information. When employees move to another department, that access is revoked.

  Confidentiality

- A technology firm maintains an alternate site that is running at all times, and operations can be moved to this location in the event of a major disaster.

- Employees need to have key cards in order to enter their company offices.

- A company hashes their data files in order to monitor whether information has been tampered with.

- Only authorized personnel at a company have write access to certain files. All other employees have only read access to these files.

Activity Instructions: Defend the CIA Triad

- A hospital only allows authorized healthcare personnel within one department access to patient Personal Identifiable Information. When employees move to another department, that access is revoked.

  Confidentiality

- A technology firm maintains an alternate site that is running at all times, and operations can be moved to this location in the event of a major disaster.

  Availability

- Employees need to have key cards in order to enter their company offices.

- A company hashes their data files in order to monitor whether information has been tampered with.

- Only authorized personnel at a company have write access to certain files. All other employees have only read access to these files.

Activity Instructions: Defend the CIA Triad

- A hospital only allows authorized healthcare personnel within one department access to patient Personal Identifiable Information. When employees move to another department, that access is revoked.

  Confidentiality

- A technology firm maintains an alternate site that is running at all times, and operations can be moved to this location in the event of a major disaster.

  Availability

- Employees need to have key cards in order to enter their company offices.

  Confidentiality

- A company hashes their data files in order to monitor whether information has been tampered with.

- Only authorized personnel at a company have write access to certain files. All other employees have only read access to these files.

Activity Instructions: Defend the CIA Triad

- A hospital only allows authorized healthcare personnel within one department access to patient Personal Identifiable Information. When employees move to another department, that access is revoked.

  Confidentiality

- A technology firm maintains an alternate site that is running at all times, and operations can be moved to this location in the event of a major disaster.

  Availability

- Employees need to have key cards in order to enter their company offices.

  Confidentiality

- A company hashes their data files in order to monitor whether information has been tampered with.

  Integrity

- Only authorized personnel at a company have write access to certain files. All other employees have only read access to these files.

Activity Instructions: Defend the CIA Triad

- A hospital only allows authorized healthcare personnel within one department access to patient Personal Identifiable Information. When employees move to another department, that access is revoked.

  Confidentiality

- A technology firm maintains an alternate site that is running at all times, and operations can be moved to this location in the event of a major disaster.

  Availability

- Employees need to have key cards in order to enter their company offices.

  Confidentiality

- A company hashes their data files in order to monitor whether information has been tampered with.

  Integrity

- Only authorized personnel at a company have write access to certain files. All other employees have only read access to these files.

  Integrity

Activity Instructions: Defend the CIA Triad

- A company employs redundant servers, which means that these systems are duplicated, and in the event of a malfunction, one server will fail over to other.

- A company's network infrastructure uses load balancers which will distribute the "load" of tasks such as file requests and data routing to a variety of servers, thereby ensuring that no single device is overburdened.

- A hacker uses a man-in-the-middle attack to intercept wireless traffic from users.

- A hacker was able to crack a hashed message and change its contents.

- A hacker launched a DDoS attack which flooded a website with unwanted traffic from a number of computers and took the site offline.

Activity Instructions: Defend the CIA Triad

- A company employs redundant servers, which means that these systems are duplicated, and in the event of a malfunction, one server will fail over to other.

  Availability

- A company's network infrastructure uses load balancers which will distribute the "load" of tasks such as file requests and data routing to a variety of servers, thereby ensuring that no single device is overburdened.

- A hacker uses a man-in-the-middle attack to intercept wireless traffic from users.

- A hacker was able to crack a hashed message and change its contents.

- A hacker launched a DDoS attack which flooded a website with unwanted traffic from a number of computers and took the site offline.

Activity Instructions: Defend the CIA Triad

- A company employs redundant servers, which means that these systems are duplicated, and in the event of a malfunction, one server will fail over to other.

  Availability

- A company's network infrastructure uses load balancers which will distribute the "load" of tasks such as file requests and data routing to a variety of servers, thereby ensuring that no single device is overburdened.

  Availability

- A hacker uses a man-in-the-middle attack to intercept wireless traffic from users.

- A hacker was able to crack a hashed message and change its contents.

- A hacker launched a DDoS attack which flooded a website with unwanted traffic from a number of computers and took the site offline.

Activity Instructions: Defend the CIA Triad

- A company employs redundant servers, which means that these systems are duplicated, and in the event of a malfunction, one server will fail over to other.

  Availability

- A company's network infrastructure uses load balancers which will distribute the "load" of tasks such as file requests and data routing to a variety of servers, thereby ensuring that no single device is overburdened.

  Availability

- A hacker uses a man-in-the-middle attack to intercept wireless traffic from users.

  Confidentiality

- A hacker was able to crack a hashed message and change its contents.

- A hacker launched a DDoS attack which flooded a website with unwanted traffic from a number of computers and took the site offline.

Activity Instructions: Defend the CIA Triad

- A company employs redundant servers, which means that these systems are duplicated, and in the event of a malfunction, one server will fail over to other.

  Availability

- A company's network infrastructure uses load balancers which will distribute the "load" of tasks such as file requests and data routing to a variety of servers, thereby ensuring that no single device is overburdened.

  Availability

- A hacker uses a man-in-the-middle attack to intercept wireless traffic from users.

  Confidentiality

- A hacker was able to crack a hashed message and change its contents.

  Integrity

- A hacker launched a DDoS attack which flooded a website with unwanted traffic from a number of computers and took the site offline.

Activity Instructions: Defend the CIA Triad

- A company employs redundant servers, which means that these systems are duplicated, and in the event of a malfunction, one server will fail over to other.

  Availability

- A company's network infrastructure uses load balancers which will distribute the "load" of tasks such as file requests and data routing to a variety of servers, thereby ensuring that no single device is overburdened.

  Availability

- A hacker uses a man-in-the-middle attack to intercept wireless traffic from users.

  Confidentiality

- A hacker was able to crack a hashed message and change its contents.

  Integrity

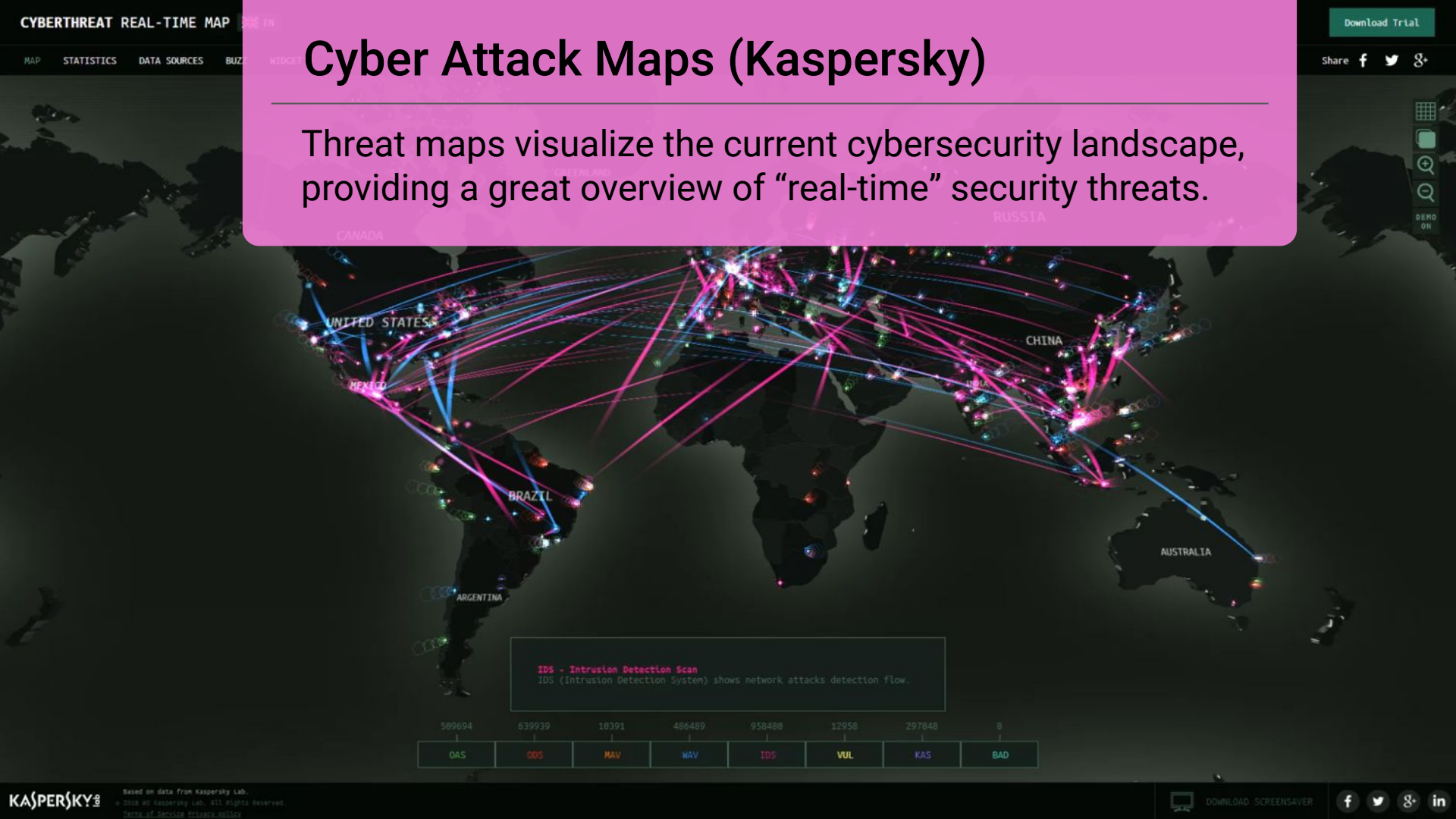
- A hacker launched a DDoS attack which flooded a website with unwanted traffic from a number of computers and took the site offline.

  Availability

Threat Landscape

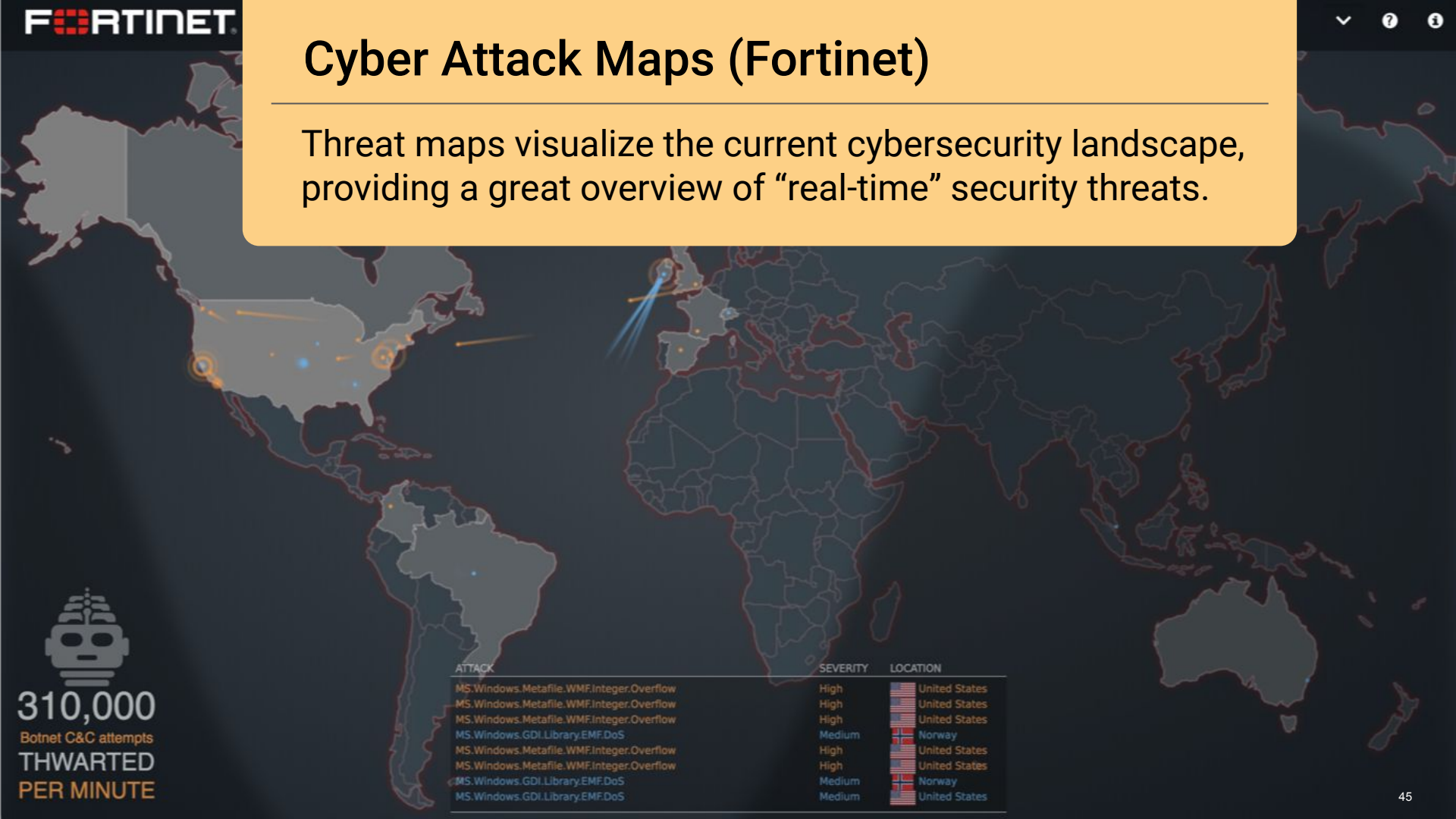
Cyber Attack Maps (Kaspersky)

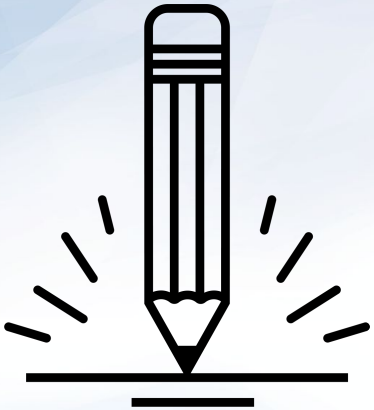
Threat maps visualize the current cybersecurity landscape, providing a great overview of “real-time” security threats.



Cyber Attack Maps (Fortinet)

Threat maps visualize the current cybersecurity landscape, providing a great overview of “real-time” security threats.





Activity: Kaspersky + Fortinet Map Exploration

In this activity, you will navigate through Kaspersky and Fortinet maps and uncover what is displayed, what terminology arises, and any visible trends.

Suggested Time:
10 minutes

Activity Instructions: Kaspersky + Fortinet Map Exploration

Instructions

Spend a few minutes exploring the Kaspersky and Fortinet Threat maps.

Maps: **Link:** threatmap.fortiguard.com
cybermap.kaspersky.com

While on these websites, answer the following questions:

1. What exactly are these websites showing?
2. Are there any terms used on these websites that you are unfamiliar with? Find and define at least three.
3. Are there any trends that stick out to you? Look for at least two.

Suggested Time: 10 Minutes

Time’s Up! Let’s Review.

Activity: Report Analysis

Threat Research

Cybersecurity and *Soft* Skills

While this program focuses primarily on the hard skills needed in cybersecurity, soft skills such as **collaboration** and **communication** are also a huge component.

Cybersecurity and *Soft* Skills

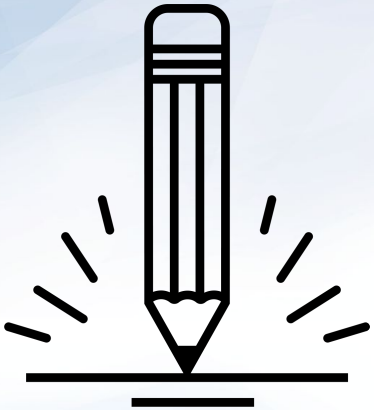
Cybersecurity often involves communicating highly technical information to a non-technical audience.

Developing your presentation skills is another critical skill. This includes public speaking, creating compelling slide visuals, and crafting a narrative for your information.

Being able to speak a common language with your audience and adjusting your message and language depending on the technical background of your audience is equally important.

In the next activity, we will work in groups of 3-4 to develop a brief presentation of a threat, vulnerability, or exploit.

We'll start these presentations today and present them in the next class.



Activity: Threat Research

In this activity, you will work in groups of three to four to research an assigned vulnerability, exploit, or threat actor.

(Instructions sent on Slack.)

Suggested Time:
40 Minutes

Activity Instructions: Threat Research

Instructions:

Form groups of three or four. You will be assigned a vulnerability, exploit, or threat actor.

Your task is to: Prepare a 5-10 minute presentation that provides an overview of the topic. Focus on answering the following question:

- What is or was the exploit, vulnerability, or threat actor?
- What damage has it done?
- What steps have or can be taken to mitigate the damage?

Notes:

- While you may be new to the field challenge yourself to “become the expert.” A huge part of being a security professional is getting up to speed quickly on technical situations using research.
- For those uncomfortable about the idea of presenting, challenge yourself to treat this as a safe place. Becoming a confident speaker is an important part of being a cybersecurity consultant that people can trust.

Suggested Time: 40 Minutes

Activity Instructions: Threat Research

Instructions

- You will continue working outside of class and create a slide presentation.
- You will give your presentations in the next class.

This is an opportunity to gain valuable research skills, security exposure, and hone your communication skills.

Suggested Time: 40 Minutes

Threat Research Presentations

1. What is this threat? (or what *was* it?)
2. What damage has it done?
3. What steps can or have been taken to mitigate?

Emotet	**Zealot Campaign**	**Digmine**	**Triton**	**BadRabbit**
Disakil	**Finfisher**	**Thrip**	**Orangeworm**	**Ploutus ATM Malware**
Gh0st RAT	**Trickbot**	**Necurs**	**BlankSlate**	**CVE-20170199**

Vulnerability, Exploits, and Threat Actors

Time’s Up! Let’s Review.

Activity: Threat Research


15:00
Break

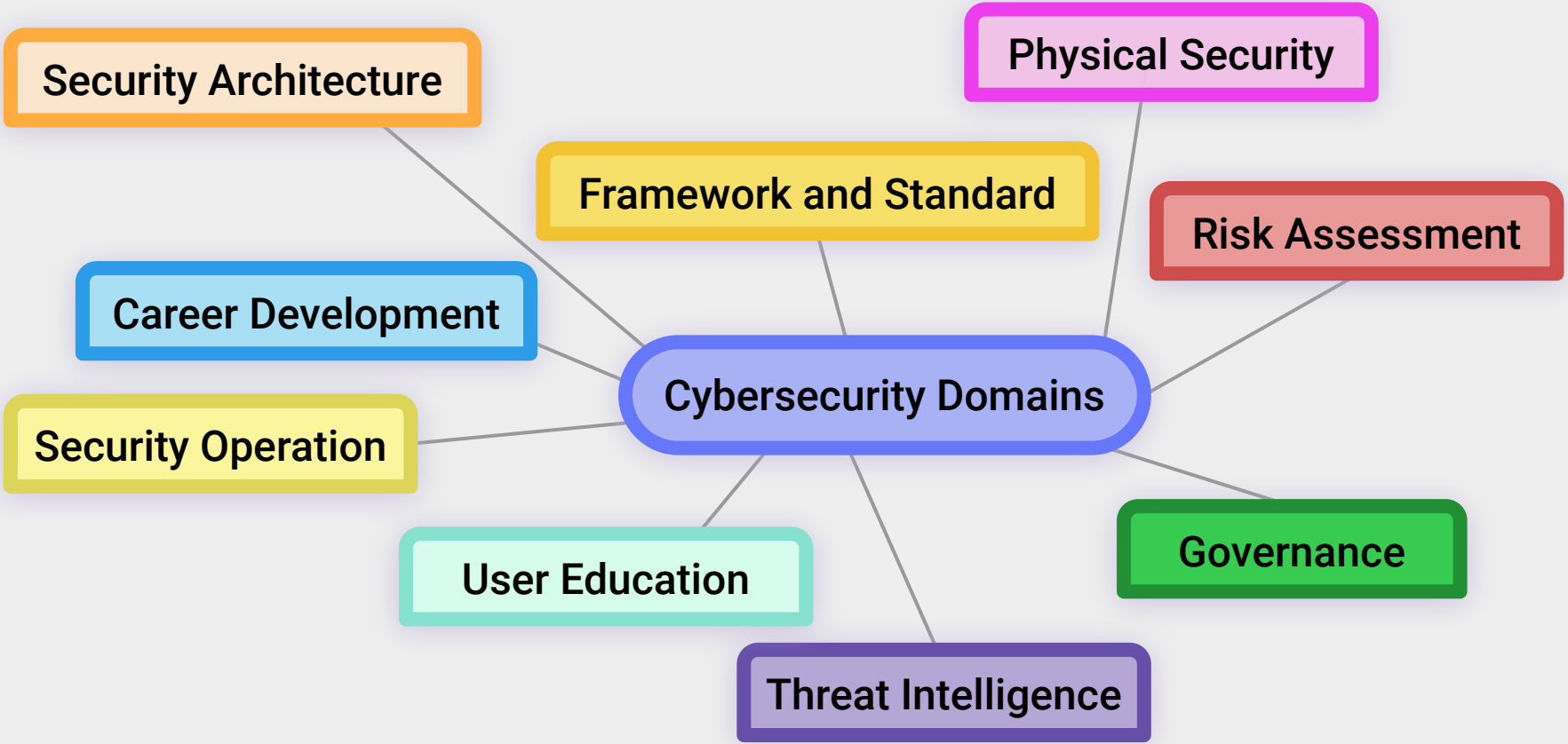
Cybersecurity Domains

Providing advice on ***getting started in digital security*** is similar to providing advice on *getting started in medicine*.

If you ask a neurosurgeon, he or she may propose some sort of experiment with dead frog legs and batteries. If you ask a dermatologist, you might get advice on protection from the sun whenever you go outside. Asking a "security person" will likewise result in many different responses, depending on the individual's background and tastes.

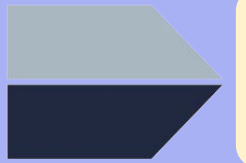
*—Tao Security's **Richard Bejtlich** on entering the cybersecurity field*

Cybersecurity Domains



Cybersecurity Domains

Security architecture: Security design that addresses the requirements and potential risks involved in a given scenario or environment. It also specifies when and where to apply security controls.

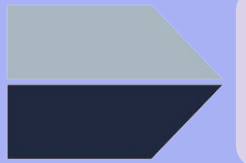


Security operations: Process of identifying, containing and remediating threats on behalf of a company or organization.

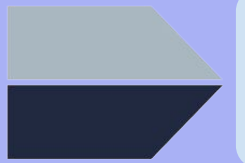
Governance: The framework for managing performance and risk, oversight of compliance and control responsibilities, and defining the cyber mission by mapping the structure, authority, and processes to create an effective program.

Cybersecurity Domains

Physical security: The protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.



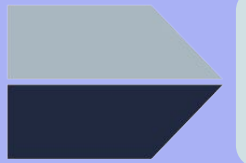
Threat intelligence: Research and analyzation of evidence-based knowledge regarding an existing or emerging menace.



Career development: The training of future cybersecurity professionals.

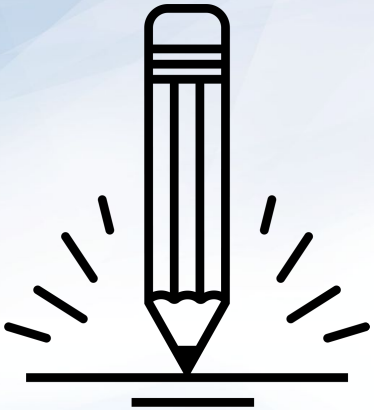
Cybersecurity Domains

Risk assessment: Analyzes what can go wrong, how likely it is to happen, what the potential consequences are, and how tolerable the identified risk is.



User education: The process of teaching users how to protect themselves from cyber attacks by informing them of risks, exploits, and external threats as well as teaching them the skills needed to combat common attacks.

Frameworks and standards: The creation of new security frameworks and practices for professionals to adhere to.



Activity: Career and Pathway Research

In this activity, we will begin to research security careers and pathways in depth.

(Instructions sent on Slack.)

Suggested Time:
10 Minutes

Activity Instructions: Career and Pathway Research

Instructions

Take a few minutes to search popular job listing websites (Indeed, LinkedIn, Dice) for cybersecurity jobs.

- Review at least three job postings in depth.
- Review at least two job postings with similar titles, and take note of differences in required skills and qualifications.

Be prepared to share:

- What search terms did you use? Why did you use these search terms?
- How confident did you feel about these search terms? Did you already have a clear idea of the specific roles you want or do you hope to have a better sense of that as the program progresses?
- How many jobs did you find?
- What did the job descriptions entail?
- What skills and qualifications did you see frequently?
- How did skills and qualifications differ between jobs with similar titles?

Suggested Time: 10 Minutes

Share Your Answers

Sample (Entry-Level) Cybersecurity Titles

Knowing the **correct** job titles and job types is the first step towards pursuing a career in the space. Be precise in your search!

Security Analyst	Security Operations Center (SOC) Analyst	Security Engineer	Systems Engineer
Cyber Threat Analyst	Cyber Defense Analyst	Incident Response Analyst	Intelligence Analyst
Information Assurance Technician	Risk Analyst	Forensics Investigator	Systems Administrator
Network Engineer	IT Auditor	Application Security Engineer	Penetration Tester
Information Analyst	Systems Security Analyst	IT Specialist	Web Engineer - Application Security

Cyber Fields by the Numbers

According to a report from Frost and Sullivan and (ISC)2 there will be **more than 1.5 million unfilled cybersecurity positions by 2020**.

From ISACA:

53% of organizations take up to six months to find qualified cybersecurity candidates.

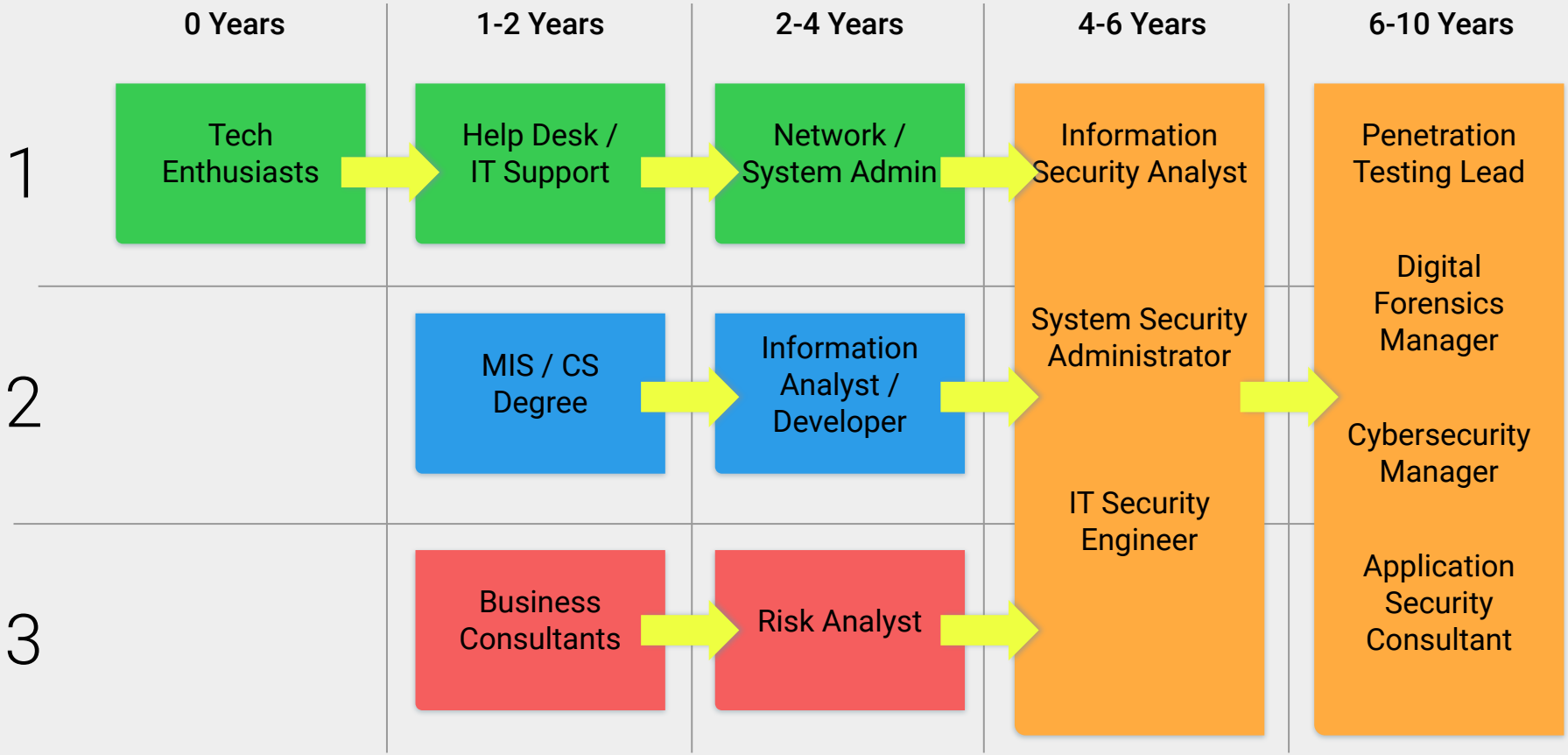
Cybersecurity jobs grew three times faster than IT jobs between 2010 and 2014.

84% of organizations believe half or fewer of its applicants for open security jobs are qualified.

From (ISC)2:

A full 87% of all cybersecurity professionals started their careers doing something different.

Career Context (Common Pathways)



Career Services Department

In class, we will tie concepts and skills in our program to career outcomes and roles. Outside of the classroom, the **Career Services** team will do the practical, hard work, helping you obtain a new role or promotion.

There are several career milestones for you to complete in Bootcamp Spot.

- You have access to them all now and can submit milestones whenever you would like.
- However, you will need to submit at least one milestone in order to unlock Career Services.
- One of the milestones, an updated, polished resume, will be a requirement in one of our later homework assignments, but you can submit this earlier if you'd like.
- Review the slides on Becoming Employer Competitive, Working with Your Profile Coach, and Working with Your Career Director.